National Security Agency
Cybersecurity Technical Report

Network Infrastructure Security Guidance

March 2022

PP-22-0266
Version 1.0

Notices and history

Disclaimer of warranties and endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Trademark recognition

Cisco® and Cisco IOS® are registered trademarks of Cisco Systems, Inc.

Publication information

Author(s)

National Security Agency
Cybersecurity Directorate

Contact information

Client Requirements / General Cybersecurity Inquiries:
Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

Media inquiries / Press Desk:
Media Relations, 443-634-0721, MediaRelations@nsa.gov

Defense Industrial Base Inquiries for Cybersecurity Services:
DIB Cybersecurity Program, DIB_Defense@cyber.nsa.gov

Purpose

This document was developed in furtherance of NSA's cybersecurity missions. This includes its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense information systems, and the Defense Industrial Base, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contents

Network Infrastructure Security Guidance i
Contents iii
1. Introduction 1
1.1 Regarding Zero Trust 1
2. Network architecture and design 2
2.1 Install perimeter and internal defense devices 2
2.2 Group similar network systems 3
2.3 Remove backdoor connections 4
2.4 Utilize strict perimeter access controls 4
2.5 Implement a network access control (NAC) solution 5
2.6 Limit and encrypt virtual private networks (VPNs) 5
3. Security maintenance 8
3.1 Verify software and configuration integrity 8
3.2 Maintain proper file system and boot management 9
3.3 Maintain up-to-date software and operating systems 10
3.4 Stay current with vendor-supported hardware 10
4. Authentication, authorization, and accounting (AAA) 11
4.1 Implement centralized servers 11
4.2 Configure authentication 12
4.3 Configure authorization 13
4.4 Configure accounting 14
4.5 Apply principle of least privilege 15
4.6 Limit authentication attempts 16
5. Administrator accounts and passwords 17
5.1 Use unique usernames and account settings 17
5.2 Change default passwords 17
5.3 Remove unnecessary accounts 18
5.4 Employ individual accounts 18
5.5 Store passwords with secure algorithms 19
5.6 Create strong passwords 21
5.7 Utilize unique passwords 22
5.8 Change passwords as needed 22
6. Remote logging and monitoring 24
6.1 Enable logging 24
6.2 Establish centralized remote log servers 25
6.3 Capture necessary log information 25
6.4 Synchronize clocks 26
7. Remote administration and network services 28
7.1 Disable clear text administration services 28
7.2 Ensure adequate encryption strength 29
7.3 Utilize secure protocols 30
7.4 Limit access to services 31

7.5 Set acceptable timeout period 31
7.6 Enable Transmission Control Protocol (TCP) keep-alive 32
7.7 Disable outbound connections 32
7.8 Remove SNMP read-write community strings 33
7.9 Disable unnecessary network services 34
7.10 Disable discovery protocols on specific interfaces 35
7.11 Network service configurations 35
7.11.1 SSH 36
7.11.2 HTTP 38
7.11.3 SNMP 39
8. Routing 39
8.1 Disable IP source routing 40
8.2 Enable unicast reverse-path forwarding (uRPF) 40
8.3 Enable routing authentication 41
9. Interface ports 42
9.1 Disable dynamic trunking 42
9.2 Enable port security 43
9.3 Disable default VLAN 44
9.4 Disable unused ports 46
9.5 Disable port monitoring 47
9.6 Disable proxy Address Resolution Protocol (ARP) 48
10. Notification banners 48
10.1 Present a notification banner 49
11. Conclusion 50
Acronyms 51
References 53
Works cited 53
Related guidance 54

Figure 1: Network perimeter with firewalls and a DMZ 3

1. Introduction

Guidance for securing networks continues to evolve as new vulnerabilities are exploited by adversaries, new security features are implemented, and new methods of securing devices are identified. Improper configuration, incorrect handling of configurations, and weak encryption keys can expose vulnerabilities in the entire network. All networks are at risk of compromise, especially if devices are not properly configured and maintained. An administrator's role is critical to securing the network against adversarial techniques and requires dedicated people to secure the devices, applications, and information on the network.

An administrator's role is critical in securing networks.

This report presents best practices for overall network security and protection of individual network devices, and will assist administrators in preventing an adversary from exploiting their network. While the guidance presented here is generic and can be applied to many types of network devices, sample commands for Cisco Internetwork Operating System (IOS) devices are provided which can be executed to implement the recommendations.

1.1 Regarding Zero Trust

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The National Security Agency (NSA) fully supports the Zero Trust security model, and much of the guidance in this report can be applied at different boundaries as recommended in Zero Trust guidance. However, this report is focused on providing guidance to mitigate common vulnerabilities and weaknesses on existing networks. As system owners introduce new network designs intended to achieve more mature Zero Trust principles, this guidance may need to be modified.

2. Network architecture and design

A secure network design that implements multiple defensive layers is critical to defend against threats and protect resources within the network. The design should follow security best practices and model Zero Trust principles, both for network perimeter and internal devices.

Apply multiple layers of defense for a more secure network design.

2.1 Install perimeter and internal defense devices

A network requires a substantial defensive strategy to protect individual components and the information they contain. Multiple layers of defense should be implemented at the network's perimeter to protect against external threats, and to monitor and restrict inbound and outbound traffic.

NSA recommends configuring and installing security devices at the perimeter of the network according to security best practices:

- Install a border router to facilitate a connection to the external network, such as an Internet service provider (ISP).
- Implement multiple layers of next-generation firewalls throughout the network to restrict inbound traffic, restrict outbound traffic, and examine all internal activity between disparate network regions. Each layer should utilize different vendors to protect against an adversary exploiting the same unpatched vulnerability in an attempt to access the internal network.
- Place publicly accessible systems and outbound proxies in between the firewall layers in one or more demilitarized zone (DMZ) subnets, where access can be appropriately controlled between external devices, DMZ devices, and internal systems.
- Implement a network monitoring solution to log and track inbound and outbound traffic, such as a network intrusion detection system (NIDS), a traffic inspector, or a full-packet capture device.
- Deploy multiple dedicated remote log servers to enable activity correlation among devices and detection of lateral movement.
- Implement redundant devices in core areas to ensure availability, which can be load-balanced to increase network throughput and decrease latency.

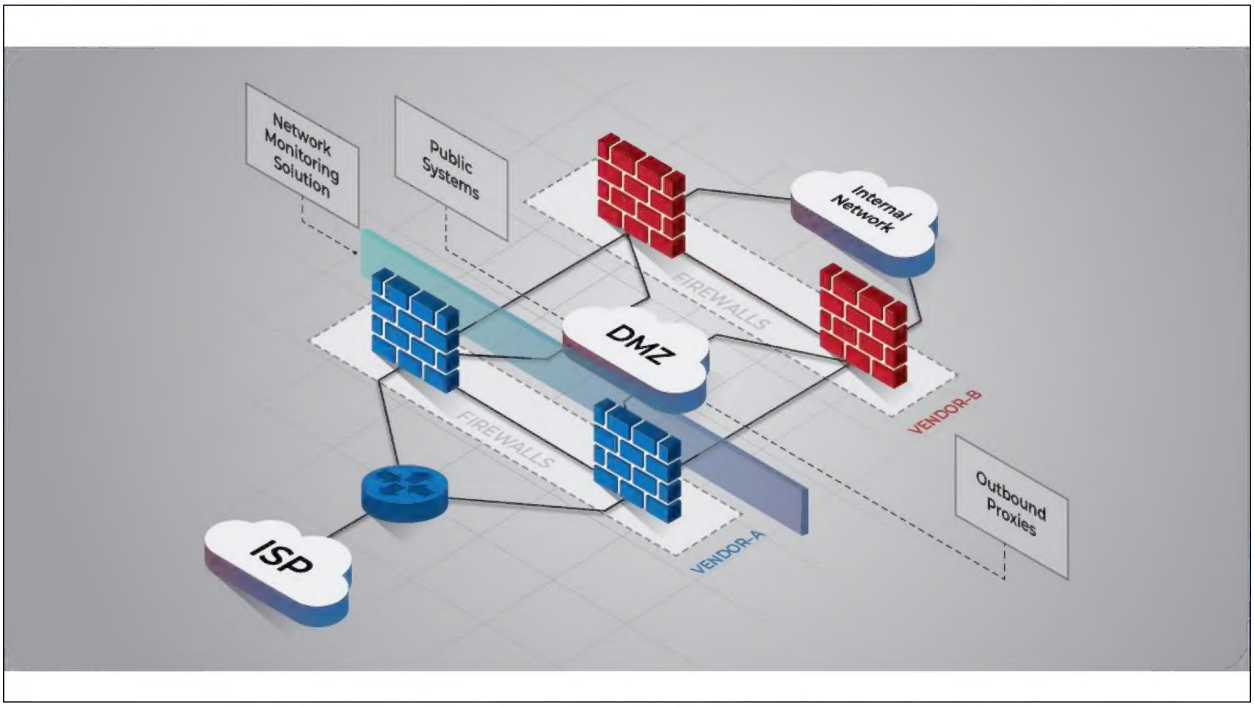

Figure 1: Network perimeter with firewalls and a DMZ

2.2 Group similar network systems

Similar systems within a network should be logically grouped together to protect against adversarial lateral movement from other types of systems. Adversaries will target systems that are more easily exploitable, such as printers, and use that initial access to further propagate to other systems on the network. Proper network segmentation significantly reduces the ability for an adversary to reach and exploit these other systems (see Cybersecurity and Infrastructure Security Agency's (CISA's) "Layering Network Security Through Segmentation" and NSA's "Segment Networks and Deploy Application-aware Defenses") [1], [2]. Additionally, access restrictions between different types of systems are easier to manage, control, and monitor if they are logically grouped together.

NSA recommends isolating similar systems into different subnets or virtual local area networks (VLANs), or physically separating the different subnets via firewalls or filtering routers. Workstations, servers, printers, telecommunication systems, and other network peripherals should be separate from each other. Operational technology, such as industrial control systems, typically need to be isolated from other information technology and high-risk networks like the Internet. This physical separation provides stronger protection because the intermediate device between subnets must be

compromised for an adversary to bypass access restrictions. Implement access restrictions on the internal routers, switches, or firewalls to allow only those ports and protocols that are required for network operations or valid mission need. Access control lists (ACLs) may need to be duplicated and applied directly to the switches to restrict access between VLANs, or they can be applied to core routers where routing is performed between internal subnets.

2.3 Remove backdoor connections

A backdoor network connection is between two or more devices located in different network areas, generally with different types of data and security requirements. If one device is compromised, an adversary can use this connection to bypass access restrictions and gain access to other areas of the network. An example of a backdoor network connection is an external border router connected to an ISP that is also directly connected to the internal or management networks. An adversary that can compromise this external border router would likely have access to the internal network, bypassing all firewalls.

NSA recommends removing all backdoor network connections and using caution when connecting devices with more than one network interface. Verify that all network interfaces of a device are at similar security levels, or that an intermediate device provides both logical and physical separation between different network areas.

2.4 Utilize strict perimeter access controls

Network perimeter devices are essential elements in a security model and should be configured to complement each other by implementing ACLs to regulate ingress and egress of network traffic. These access control rulesets should be configured to explicitly allow only services and systems that are required to support the mission of the network. If firewalls and perimeter routers are not configured with adequate network security policies, it will permit unnecessary access to or from the internal network and increase the risk of network compromise and information gathering.

NSA recommends carefully considering which connections to allow, and creating rulesets that focus on only permitting those allowed and denying everything else. This method allows a single rule to deny several types of connections, instead of needing to create a separate rule for each blocked connection. If it is necessary to dynamically apply additional perimeter rulesets to prevent exploitation attempts from being

completed or continuing, NSA recommends the use of an intrusion prevention system (IPS).

NSA also recommends enabling logging on these rulesets to include, at a minimum, all that deny or drop network traffic and including successful or unsuccessful administrator access to critical devices.

2.5 Implement a network access control (NAC) solution

An adversary who wishes to gain internal access to a network must either find a way through the external perimeter of the network or obtain access from inside the network. A NAC solution prevents unauthorized physical connections and monitors authorized physical connections on a network.

NSA recommends implementing a NAC solution that identifies and authenticates unique devices connected to the network. Port security is a mechanism that can be implemented on switches to detect when unauthorized devices are connected to the network via a device's media access control (MAC) address. However, port security can be difficult to manage. For example, it increases the number of support tickets due to valid blocked network ports (e.g., connected devices that change often, such as conference rooms). In addition, adversaries who can spoof a MAC address can bypass it as well. A more robust solution utilizes 802.1X, which authenticates devices based on a trusted digital certificate installed on the device. While it is more difficult to implement, due to the generation and installation of certificates, it is easier to manage than port security and offers a higher level of assurance.

2.6 Limit and encrypt virtual private networks (VPNs)

VPN gateways tend to be accessible from the Internet and are prone to network scanning, brute force attempts, and zero-day vulnerabilities. To mitigate many of these vulnerabilities, administrators should disable all unneeded features and implement strict traffic filtering rules for traffic flowing to VPN gateways [2].

NSA recommends limiting VPN gateway access to User Datagram Protocol (UDP) port 500, UDP port 4500, Encapsulating Security Payload (ESP), and other appropriate ports as needed. When possible, limit accepted traffic to known VPN peer Internet Protocol (IP) addresses. Remote access VPNs cannot be added to a static filtering rule if the remote peer IP address is unknown. If traffic cannot be filtered to specific IP

addresses, use an IPS in front of the VPN gateway to monitor for malformed IP Security (IPsec) traffic and inspect IPsec session negotiations.

All IPsec VPN configurations require an IPsec policy and an Internet Key Exchange (IKE) policy. These policies determine how it will negotiate each phase when establishing the IPsec tunnel. If either phase is configured to allow weak cryptography, the entire VPN may be at risk and data confidentiality will be lost. Each IKE policy includes at least three key components:

1. Diffie-Hellman algorithm/group
2. Encryption algorithm
3. Hashing algorithm

The following is the minimum recommended settings per Committee on National Security Systems Policy (CNSSP) 15:

- Diffie-Hellman Group: 16 with 4096 bit Modular Exponent (MODP)
- Diffie-Hellman Group: 20 with 384 bit elliptic curve group (ECP)
- Encryption: Advanced Encryption Standard (AES)-256
- Hash: Secure Hash Algorithm (SHA)-384

Diffie-Hellman Group 15 is also acceptable based on the minimum requirements of CNSSP 15, but Group 15 is not recommended due to interoperability issues that have been observed.

A VPN tunnel can be established between two endpoints to provide an encrypted communication channel over an untrusted network, such as the Internet. When establishing a VPN proposal, policy, or transform-set, ensure it follows CNSSP 15 recommendations [4]. The CNSSP 15 requirements are explained in the draft Internet Engineering Task Force (IETF) document on "Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec)" [5].

To ensure they are not inadvertently used, disable the default polices and proposals for Internet Security Association and Key Management Protocol (ISAKMP) and IKEv2 with the following configuration commands:

```
no crypto isakmp default policy
```

```
no crypto ikev2 policy default

no crypto ikev2 proposal default

no crypto ipsec transform-set default
```

Note: If the default policies are disabled, only the explicitly configured policies will be used.

Establish an IKEv2 proposal, policy, and profile with the following example configuration commands:

```
crypto ikev2 proposal <IKEV2_PROPOSAL_NAME>
 encryption aes-gcm-256
 group [16|20]

crypto ikev2 policy <IKEV2_POLICY_NAME>
 proposal <IKEV2_PROPOSAL_NAME>

crypto ikev2 profile <IKEV2_PROFILE_NAME>
 match identity remote ...
 authentication remote ...
 authentication local ...
```

The configuration of the profile will depend on the network it is configured for, and must have local and remote authentication methods and a `match` statement. A separate keyring can also be established and applied to the profile for multiple pre-shared keys.

Establish an IPsec transform-set with the following example configuration commands:

```
crypto ipsec transform-set <IPSEC_TRANSFORM_NAME> esp-gcm 256
 mode tunnel
```

Establish an IPsec profile, which utilizes the IKEv2 profile and IPsec transform-set defined above, with the following example configuration commands:

```
crypto ipsec profile <IPSEC_PROFILE_NAME>
 set transform-set <IPSEC_TRANSFORM_NAME>
 set pfs group16
 set ikev2-profile <IKEV2_PROFILE_NAME>
```

The IPsec profile should be applied to the tunnel interface with the following configuration commands:

```
interface <TUNNEL_INTERFACE_NAME>
 tunnel protection ipsec profile <IPSEC_PROFILE_NAME>
 no shutdown
```

For more information, refer to "Configuring IPsec Virtual Private Networks," "Mitigating Recent VPN Vulnerabilities," and "Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations" [6], [7], [8].

Return to Contents

3. Security maintenance

Outdated hardware and software may contain publicly known vulnerabilities and provide an easy mechanism for adversaries to exploit the network. These vulnerabilities are mitigated by regularly upgrading the hardware and software to newer versions that are supported by the vendor. Additionally, the integrity of downloaded software should be verified before and during use. Security maintenance should be performed on a regular basis to ensure devices continue to operate securely.

Upgrade hardware and software to ensure efficiency and security.

3.1 Verify software and configuration integrity

An adversary can introduce malicious software into network devices by modifying operating system files, the executable code running in memory, or the firmware or bootloader that loads the operating system of a network device. Software that has been maliciously modified on a network device can be used by an adversary to violate data integrity, exfiltrate sensitive information, and cause a denial of service (DoS).

NSA recommends verifying the integrity of operating system files installed and running on devices by comparing the cryptographic hash of the file with the known good hash published by the vendor. When upgrading operating system files, perform the same integrity verification on the files prior to and after installation to ensure no modifications were made. A basic online hash can be computed on an operating system image file with the following exec command:

```
verify /sha512 <PATH:filename>
```

Older devices may only support a Message Digest 5 (MD5) hash, which can be computed with the following exec command:

```
verify /md5 <PATH:filename>
```

The computed hash can be compared with the information published for the file on the Support pages of https://www.cisco.com/ [9]. More information on network device verification is available in the "Network Device Integrity (NDI) Methodology," "Network Device Integrity (NDI) on Cisco IOS Devices," and "Validate Integrity of Hardware and Software" documents [10], [11], [12].

Rather than performing these more complex software modifications, an adversary may choose to simply change the configuration. Configuration changes can be a sign that a device has been compromised.

NSA also recommends implementing a configuration change control process that securely creates device configuration backups to detect malicious modifications. When a configuration change is needed, document the change and include the authorization, purpose, and mission justification. Periodically verify that modifications have not been applied by comparing current device configurations with the most recent backups. If suspicious changes are observed, verify the change was authorized.

3.2 Maintain proper file system and boot management

Many network devices have at least two different configurations, one or more saved in persistent storage and an active copy running in memory. Permanent changes to the configuration should be saved or committed to prevent configuration inconsistencies if the device is rebooted or loses power. Configuration changes can be saved on a device with the following exec command:

```
copy running-config startup-config
```

If changes are meant to be temporary, NSA recommends inserting comments before the updated configuration lines to include why it was made and when it can be removed, and removing the comments and temporary changes at the appropriate time. If the device does not support comments, insert comments in a backup copy of the configuration to compare with the version on the device. Use an encrypted protocol when copying configurations remotely, such as Secure File Transfer Protocol (SFTP) or

Secure Copy Protocol (SCP). This mechanism to backup or archive configurations, and the backup repository, must be protected from unauthorized access.

NSA also recommends checking for unused or unnecessary files on each device and removing them with the following exec commands:

```
dir /recursive all-filesystems

delete <PATH:filename>
```

Older operating system files or outdated backup configuration files stored on the device are most likely unnecessary, and should be removed. Storing multiple versions of software provides an adversary the opportunity to reload outdated software and reintroduce vulnerabilities patched in newer versions of the operating system.

3.3 Maintain up-to-date software and operating systems

Maintaining up-to-date operating systems and stable software protects against critical vulnerabilities and security issues that have been identified and fixed in newer releases. Devices running outdated operating systems or vulnerable software are susceptible to a variety of published vulnerabilities, and exploiting these devices is a common technique used by adversaries to compromise a network.

NSA recommends upgrading operating systems and software on all devices to the latest stable version available from the vendor. Upgrading the operating system may require additional hardware or memory upgrades, and obtaining a new software version may require a maintenance or support contract with the vendor. Most network infrastructure devices do not support an auto-update feature, so it is necessary to implement a requisition and installation process for the latest software with the vendor.

For a list of the most recent Cisco operating system files, see the Support pages at https://www.cisco.com/ [9].

3.4 Stay current with vendor-supported hardware

Vendors eventually stop supporting specific hardware platforms and, if a failure occurs, these end-of-life devices cannot be serviced. In addition to device instability and memory requirement concerns, there is an increased risk of an adversary exploiting the device due to a lack of software updates to fix known vulnerabilities. Newer, vendor-

supported hardware platforms have improved security features, including protection from known vulnerabilities.

Once a vendor publishes an end-of-life notice or announces that a device will no longer be supported, NSA recommends constructing a plan to upgrade or replace affected devices with newer equipment, according to vendor recommendations. Outdated or unsupported devices should be immediately upgraded or replaced to ensure the availability of network services and security support.

For a list of supported Cisco devices, see the Support pages at https://www.cisco.com/ [9].

Return to Contents

4. Authentication, authorization, and accounting (AAA)

Centralized AAA servers provide a consolidated mechanism to manage administrative access to devices, and the accounts created are more challenging for an adversary to compromise since credentials are not stored directly on devices. Properly configuring these servers provides an authoritative source for managing and monitoring access, improves consistency of access control, reduces configuration maintenance, and reduces administrative costs. All devices should first be configured to use modern AAA services with the following configuration example command for Cisco IOS devices:

Control access and reduce maintenance through use of AAA.

```
aaa new-model
```

Applying the above configuration ensures a device will not use legacy authentication and authorization methods.

4.1 Implement centralized servers

All devices should be configured to use centralized AAA servers. NSA recommends implementing at least two AAA servers on the network to ensure availability, and assist with detection and prevention of adversary activities. If one server becomes unavailable

due to scheduled maintenance or for other reasons, the remaining servers will continue providing the centralized AAA services. The servers should be:

- Configured to authenticate devices with a unique and complex pre-shared key to ensure only authorized devices can use the AAA services (see 5.6 Create strong passwords).
- Configured to use the same protocol (e.g., TACACS+, RADIUS, or LDAP) for consistency, and use encrypted transport when supported (e.g., RadSec, Diameter, LDAPS, or IPsec encapsulated).
- Synchronized with each other to ensure consistency of user credentials and access controls.

A server group with multiple AAA servers can be configured with the following configuration commands:

```
aaa group server {tacacs+ | radius | ldap} <GROUP_NAME>
 server-private <IP_ADDRESS_1> key <KEY_1>
 server-private <IP_ADDRESS_2> key <KEY_2>
```

Some older devices may utilize the keywords `tacacs-server` and `radius-server` in the configuration, which prevents assigning a unique key to each server.

NSA recommends replacing these lines with the above configuration format, and assigning a unique pre-shared key to each server. If an adversary obtains the pre-shared key to one server, the key needs to be revoked, but other servers with different keys can continue to be used by the devices.

4.2 Configure authentication

Authentication verifies the identity of a person or entity. All devices should be configured to use centralized servers for AAA services first, and local administrator accounts as a backup method only if all the centralized servers are unavailable. The same applies to privileged level authentication; devices should only use the local privileged level password if all centralized servers are unavailable. This order of precedence will prevent an adversary, who obtains local administrator account credentials, from logging into the devices since access will usually be controlled by the AAA servers.

NSA recommends configuring centralized authentication for `login` and `enable` (privileged) access as the primary method, as shown in the following configuration commands:

```
aaa authentication login default group <GROUP_NAME> local
aaa authentication enable default group <GROUP_NAME> enable
```

Using the `default` keyword ensures the configuration is applied globally in all instances when an explicit authentication list is not specified. If a custom named list is used instead, it would be necessary to explicitly apply this list to all instances where AAA is used and potentially leave some management services incorrectly configured and open to compromise. The `default` list is always applied when a custom named list is not explicitly applied.

The *<GROUP_NAME>* should be the custom name of the AAA server group (defined previously) that includes the IP addresses of the centralized AAA servers and their associated keys.

The `line` keyword should not be used as these passwords are not securely stored in the configuration and do not provide accountability.

The `none` keyword should never be used since it disables authentication.

4.3 Configure authorization

Authorization validates that a person or entity has permission to access a specific resource or perform a specific action. The organization, situation, and device purpose will dictate authorized administrator commands. At the least, authorization should be applied to starting an exec session (shell) and execution of other shell commands, including configuration commands.

NSA recommends adequately restricting what legitimate administrators are authorized to execute to prevent an adversary from performing unauthorized actions with a compromised account. Most administrators use privilege level 1 for user level access and privilege level 15 for privileged level access. Authorization should be applied to both of these levels and any other privilege levels used by administrators with the following configuration commands:

```
aaa authorization exec default group <GROUP_NAME> local
```

```
aaa authorization commands 1 group <GROUP_NAME> local
aaa authorization commands 15 group <GROUP_NAME> local
aaa authorization config-commands
```

The `default` list should be used to ensure the configuration is applied everywhere.

The *<GROUP_NAME>* should be the custom name of the AAA server group (defined previously) that includes the IP addresses of the centralized AAA servers and their associated keys.

If desired, the `if-authenticated` keyword can be applied after the `local` keyword. If an administrator is successfully logged in and all the centralized AAA servers become unavailable, they will no longer be authorized to execute commands. The `if-authenticated` keyword ensures an authenticated user will continue to be authorized to execute commands. However, be cautious with this keyword as it could potentially give an administrator access beyond what is configured on the centralized AAA servers.

The `none` keyword should never be used since it disables authorization.

4.4 Configure accounting

Accounting keeps records of all relevant resources accessed or actions performed, holding administrators accountable. Waiting until an event is stopped to generate an accounting record is insufficient, as a particular action could take an unreasonable amount of time to complete before the record is generated. Accounting records can be collected for several other event types, but is dependent on the organization and purpose of devices.

NSA recommends that system configuration changes be centrally recorded, and a process implemented to periodically review these records to detect potential malicious activities. At a minimum, accounting records should be collected when an exec session (shell) is started and stopped, and when shell commands are started and stopped. Similar to authorization, accounting of `commands` must be applied to all administrator privilege levels with the following configuration commands:

```
aaa accounting exec default start-stop group <GROUP_NAME>
aaa accounting commands 1 default start-stop group <GROUP_NAME>
aaa accounting commands 15 default start-stop group <GROUP_NAME>
```

The `default` list should be used to ensure the configuration is applied everywhere.

The *<GROUP_NAME>* should be the custom name of the AAA server group (defined previously) that includes the IP addresses of the centralized AAA servers and their associated keys.

4.5 Apply principle of least privilege

Least privilege is a security concept that authorizes access to a person or entity at the lowest privilege level necessary to perform authorized tasks. Many common tasks do not require privileged level access, such as viewing status of network interfaces or reviewing routing tables. To implement least privilege, administrators should initially login with the lowest privilege level necessary. This provides an additional layer of security that an adversary must circumvent to fully compromise a device. It also prevents administrators from inadvertently making configuration changes to a device.

NSA recommends that all accounts be configured with privilege level 1 or 0, and require administrators to enter additional credentials to elevate to a higher privilege level to perform required tasks. Privilege levels should be periodically reviewed, and unnecessary accesses removed to prevent inadvertent use of privileged level commands at lower privilege levels.

The privilege level of individual local accounts can be changed with the `privilege` keyword. Assign local accounts to privilege level 1 with the following configuration command:

```
username <USER_NAME> privilege 1
```

Note: This does not change the account password.

All administrator accounts logging in at privilege level 1 will be required to execute the `enable` command and provide additional credentials to elevate to a higher privilege level. In addition to reviewing all local administrator accounts and ensuring they are assigned the least privilege level, it is also necessary to review all accounts configured on the centralized AAA servers.

Similarly, the same concept should be applied to the console (CON), auxiliary (AUX), and virtual teletype (VTY) lines. When AAA authorization is properly configured, it should not be dependent on the configuration of the lines. However, it is a best practice

to ensure the lines are configured to the least privilege level with the following configuration commands:

```
line con 0
 privilege level 1

line aux 0
 privilege level 1

line vty 0 4
 privilege level 1

line vty 5 15
 privilege level 1
```

Depending on the device, it may be necessary to apply a similar configuration to other lines as well. If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands.

4.6 Limit authentication attempts

Limiting the number of authentication attempts and introducing a login delay prevents an adversary from performing brute force password cracking against a device in an attempt to obtain access.

NSA recommends restricting failed remote administration attempts to a maximum of three or less with the following configuration example command for Cisco IOS devices:

```
aaa authentication attempts login 3
```

Similarly, the same concept of three or less failed attempts should be applied to Secure Shell (SSH) sessions with the following configuration command:

```
ip ssh authentication-retries 3
```

NSA also recommends introducing a delay of at least one second between login attempts to significantly slow down brute force attempts with the following configuration command:

```
login delay 1
```

Return to Contents

5. Local administrator accounts and passwords

Local accounts are vital to the management of network devices. If centralized authentication fails, the local accounts provide administrators with access to the network devices to troubleshoot and diagnose network issues. Local accounts should be unique, authenticated with a unique and complex password, and provide accountability for individual administrators. If a password policy does not exist for the organization, establish and enforce a new policy. Periodically review and revise the policy, when necessary.

Create unique local accounts with complex passwords.

This section focuses primarily on local accounts and passwords. Traditional network devices use legacy methods for managing local accounts, and they may not support the recommended mechanisms for composing, changing, and verifying passwords. The simplistic nature of these local accounts requires different recommendations to be applied. This is in contrast to the centralized AAA servers where multi-factor authentication, password complexity, previous password comparison, and other concepts can be properly implemented.

5.1 Use unique usernames and account settings

Most devices have default administrative credentials which are advertised to the public, and they often grant full administrative access to a device. Maintaining these settings offers the adversary an easy entry into the network to connect and potentially gain privileged level access to anonymously monitor or reconfigure the device.

NSA recommends removing all default configurations and reconfiguring each device with a unique and secure account for each administrator. Do not introduce any new devices into the network without first changing the default administrative settings and accounts. Note that the default user account on some devices cannot be removed.

5.2 Change default passwords

Most devices are assigned a default password, or sometimes no password, to allow an administrator easy access prior to initial configuration. Many of these passwords are public knowledge and typically do not need to be changed for the device to work properly. They are prime targets for malicious automated scanners (botnets) to exploit, as the default credentials provide privileged level access to the device.

NSA recommends removing all default passwords and assigning a unique, complex, and secure password to all levels of access, including both user and privileged levels. Additionally, when introducing new devices into the network, change the default user and privileged level passwords before attaching the device to the network.

5.3 Remove unnecessary accounts

Some devices have accounts that are not needed. Since they may be rarely used or not used at all, maintaining their security is often overlooked. If possible, rename or remove default accounts that are not associated with a particular administrator.

NSA recommends that the number of accounts authorized to log onto devices should be limited to what is necessary; all others should be removed. When an administrator leaves an organization or changes roles, the associated accounts should be disabled or removed. On Cisco IOS devices, remove a local account with the following configuration command:

```
no username <NAME>
```

5.4 Employ individual accounts

Accounts can be used by individual administrators or shared among a group. However, if multiple administrators use a group account to access the device, accountability cannot be enforced as configuration changes will not be associated to a specific individual. For this reason, adversaries target group accounts to gain unauthorized access to devices.

NSA recommends disabling all shared or group administrator accounts, and using a unique account for each administrator to provide access for configuration changes and to ensure accountability on each device. If group accounts are necessary, NSA recommends monitoring these accounts to detect any suspicious activity. It may not be feasible to create a backup local account for each administrator, but a single group account known to every administrator does not provide individual accountability.

NSA also recommends that local accounts only be used in emergency situations when the centralized AAA servers are unavailable. During such an event, unique local emergency account passwords should be maintained by a trusted individual who does not have direct access to the devices. Administrators can request the local account and password and, once the emergency situation has ended, the trusted individual can then

change the password. This will prevent password reuse and ensure accountability. All other authentication requests should occur via the centralized AAA servers.

5.5 Store passwords with secure algorithms

Passwords are generally stored in the configuration of a device or in a local database, as clear text, encrypted, or a one-way hash. Clear text should never be used, and some encryption or hash functions are considered weak and could easily be broken using publicly available tools. An adversary could accumulate passwords or hashes from the configuration or local database by using a network analyzer or by compromising a central management system that stores configuration files. The clear text and weak algorithm passwords could be easily cracked and used to obtain user or privileged level access to a device. Cisco IOS supports the following one-way hash and encrypted types:

- **Type 0** passwords should not be used because they are stored in clear text
- **Type 4** password hashes should not be used because they are easy to crack
- **Type 5** (MD5) password hashes should be avoided except on older operating systems that do not support Types 6, 8, or 9
- **Type 6** passwords are AES-encrypted and should only be used for passwords that need to be encrypted instead of hashed (such as for VPN keys), or on systems that do not support Type 8 (which typically implies that Type 9 is also unavailable)
- **Type 7** passwords should not be used because they are easily reversible, even though they are encrypted
- **Type 8** (SHA-256 PBKDF2) password hashes are recommended
- **Type 9** (Scrypt) password hashes are not approved by the National Institute of Standards and Technology (NIST)

For more information on the above password types, see Cisco Password Types: Best Practices [13].

NSA recommends that all passwords on a device be stored using the most secure algorithm available, and never stored as clear text. One-way hash algorithms are irreversible and generally should be used for storing passwords. However, if one-way hash algorithms are unavailable, the passwords should be encrypted with a strong unique key.

When creating a user account or assigning a password, some devices require the algorithm to be specified. Special attention should be given to privileged level accounts, but this guidance also applies to user accounts, management ports, authenticated routing protocols, VPN keys, and any place where a password may be specified in the device's configuration.

Prevent clear text passwords with the following configuration command:

```
service password-encryption
```

Store a Type 8 password hash for a local account with the following configuration command:

```
username <NAME> algorithm-type sha256 secret <PASSWORD>
```

Note that the `algorithm-type` keyword is not stored in the saved configuration in `nvram:/startup-config`; instead the `secret` keyword is replaced with `secret 8` prior to the hashed password.

If reversible encrypted passwords are needed (such as for VPN keys), use Type 6 AES instead of Type 7 passwords with the following configuration commands:

```
password encryption aes
key config-key password-encrypt <KEY>
```

The *<KEY>* should be a unique and complex password that is used to generate the key to encrypt Type 6 passwords. It should not be a default, weak, or easily guessable password, and should not be reused elsewhere in the configuration. An adversary that guesses this key could use it to decrypt all Type 6 passwords stored in the configuration. Once this key is set, it generally does not need to be retained.

Note: The `key config-key password-encrypt` configuration command is not stored in the saved configuration in `nvram:/startup-config`.

Since it does not need to be retained, NSA recommends using a unique key for every device which will prevent an adversary from using the same key to decrypt the Type 6 passwords on all of the devices. Note that if the key is ever changed, the Type 6 encrypted passwords will need to be manually set again.

5.6 Create strong passwords

A device configured with a weak password increases an adversary's ability to compromise that device. An adversary may be able to easily guess a weak password or crack it using publicly available password cracking tools (e.g., dictionary or brute force attempts). Once privileged level access is obtained, an adversary can make configuration changes that potentially compromise other devices on the network.

NSA recommends assigning a unique and complex password to all levels of access, including both user and privileged level accesses. Unique and complex passwords should also be used for routing authentication, time synchronization, VPN tunnels, Simple Network Management Protocol (SNMP) community strings, and anywhere else passwords are stored in the configuration. Passwords should meet the following complexity requirements:

- Use all the different character classes (uppercase, lowercase, numbers, and special characters)
- Be at least fifteen characters long
- Not based on unmodified words or acronyms
- Not be a keyboard walk
- Not same as username
- Not related to the network, organization, location, local sports team, or other function identifiers
- Not identical or similar to the last password or passwords assigned elsewhere
- Not a default, blank, or publicly known password

An organization's password policy may not require passwords managed through the centralized AAA servers to adhere to all of these recommendations, especially when coupled with multi-factor authentication and other principals. The above guidance should at least be applied to local accounts and other passwords that are stored in the configuration of a network device, where centralized security controls cannot be applied.

NSA highly discourages the use of SNMP version 1 or 2c. For more information, refer to 7.1 Disable clear text administration services and 7.8 Remove SNMP read-write community strings.

An adversary with knowledge of the network, location, programs, etc. could easily guess (or know) these terms, thus aiding them in cracking the passwords.

NSA also recommends checking for weak passwords on a regular basis to enforce the organization's password policy. Password complexity should be checked before setting a new password, and network administrators should periodically review network device configurations to identify the use of weak password algorithms.

5.7 Utilize unique passwords

Assigning the same password to multiple accounts or multiple levels of access could impact accountability and authorization. If an administrator accesses the device via an unencrypted protocol, an adversary could use a network analyzer to collect the password from network traffic. If an adversary gains user level access, they could potentially reuse the same password to also gain privileged level access.

Assigning the same password to multiple devices allows an adversary to compromise numerous devices at the same time, without any extra effort. If the same password was assigned to a majority of the devices, an adversary would only need to compromise a single password to obtain privileged level access to all of those devices.

NSA recommends assigning a unique, complex, and secure password for each account and privileged level on each device.

NSA also recommends checking for password reuse across multiple accounts and levels of access, and across multiple devices. Identical hashes can be an indication of password reuse.

5.8 Change passwords as needed

Periodically changing passwords has historically led to the use of weaker passwords, and enforcing this policy may not be necessary if users follow the guidance in 5.6 Create strong passwords. The initial creation of strong passwords is a more effective method of reducing successful password compromises.

NSA recommends changing a password immediately if the password or password hash has been compromised, and storing it securely as described in 5.5 Store passwords with secure algorithms. Given enough time and resources, every password can be guessed or brute force cracked, which is an attempt at all possible character

combinations. Compromised passwords that have not been changed give an adversary even more time to use these techniques. Additionally, if an adversary eventually cracks an old password, they may continue attempting variations and guess the current password if it was based on a previous password.

Unfortunately, it can be difficult to discern when a password has been compromised, especially local passwords stored in the configuration. Traditional network devices are significantly more simplistic in how they store and transmit the configuration, which includes passwords and password hashes. Furthermore, emailing network device configurations or storing them in unprotected file shares could constitute a compromise, because the passwords and password hashes stored in the configurations are left unprotected. Additionally, passwords stored with a weak algorithm should be considered compromised, since they are significantly easier to crack.

If the confidentiality of passwords cannot be maintained or the organization desires to regularly attempt to evict actors who may have compromised passwords without being detected, NSA recommends establishing an aging policy that incorporates changing passwords on a regular basis. Changing local passwords can be significantly more cumbersome than centralized passwords, so it is necessary to choose a time frame that is reasonably practical for network administrators to follow, while reducing the amount of time an adversary can utilize a potentially compromised password. If the device does not support long passwords, it is recommended that passwords be changed more frequently to prevent an adversary from cracking a password that is still in use.

Note: If a password is stored using a convoluted Type 9 secret where the `secret 9` password hash begins with `$14$`, it indicates that the password was not recently changed. The password hash was converted from Type 5 during a previous operating system upgrade. The convoluted Type 9 secret should be removed by changing the password to a Type 8 secret with the `algorithm-type sha256` keywords, as previously described in 5.5 Store passwords with secure algorithms.

Return to Contents

6. Remote logging and monitoring

Logging is an important mechanism for recording device activities and tracking network security events, providing administrators with the ability to review the logs for suspicious activities and to investigate incidents. An incomplete logging configuration on a device can lead to missing or inaccurate information and difficulty correlating events that occurred on a device or the network. Proper logging includes sending logs to multiple remote log servers, synchronizing the clock to multiple authenticated time sources, and implementing log management policies and procedures. A security information and event management (SIEM) system can be used to aggregate and analyze logs received by the remote log servers. Logs should be retained as recommended by the Office of Management and Budget (OMB) Memorandum M-21-31 [14].

Enable and configure logging to identify malicious activity.

6.1 Enable logging

Log messages will only be generated on network devices when logging is enabled. Devices should be configured to send log messages to a local log buffer and centralized log servers simultaneously.

NSA recommends enabling syslog logging, setting the local log buffer to 16 megabytes or greater, and establishing a procedure to verify the logs are received and reviewed on a regular basis. Most devices should be able to support the larger buffer size, but it can be decreased for a particular device if there is insufficient memory.

Ensure that syslog logging is enabled with the following configuration command:

```
logging on
```

Increase the maximum local log buffer with the following configuration command:

```
logging buffered 16777216 informational
```

Note: This will also change the logging level to informational, as both values must be set simultaneously.

6.2 Establish centralized remote log servers

Log messages sent to remote log servers are less vulnerable to compromise or erasure, ensuring that the messages will not be impacted in the event a device is compromised, rebooted, or the local log buffer becomes full. Multiple log servers are critical when defending against DoS effects and reducing a single point-of-failure.

NSA recommends establishing at least two remote, centralized log servers to ensure monitoring, redundancy, and availability of device log messages. If supported, ensure the log messages are encrypted in transit to prevent unauthorized disclosure of sensitive information. Outbound syslog messages can only be encrypted on a Cisco IOS device by creating an IPsec tunnel between the device and the remote syslog servers, as described in 2.6 Limit and encrypt virtual private networks (VPNs). Configure at least two remote log servers with the following configuration commands:

```
logging host <IP_ADDRESS_1>
logging host <IP_ADDRESS_2>
```

6.3 Capture necessary log information

Devices configured with sufficient information in the logs provide administrators with the information they need to analyze events related to an incident, including correlating multiple events or events occurring on other devices.

NSA recommends setting the trap and buffer logging levels on each device to at least syslog level "informational" (code 6) to collect all necessary information. Devices can be configured for "debugging" (code 7), but the increased number of generated messages may slow down the log review process. Set both the trap and buffer logging levels to informational with the following configuration commands:

```
logging trap informational
logging buffered 16777216 informational
```

Note that this will also set the maximum size of the local log buffer, as both values must be set simultaneously.

Logging can also be enabled on the console and VTY lines with the `console` and `monitor` keywords, respectively. These methods will immediately alert administrators that are logged in, but the messages are not retained. It is not necessary to enable

logging for these methods unless it is desired by the administrators. They can be disabled with the following configuration commands:

```
no logging console
no logging monitor
```

NSA also recommends using Coordinated Universal Time (UTC) for the time zone, especially if the network spans multiple time zones. All log messages should contain a properly configured timestamp with the full date including the year, the time including seconds and milliseconds, and the time zone. Ensure the time zone is properly set and enable all the features listed above with the following configuration commands:

```
clock timezone UTC 0 0
service timestamps log datetime msec localtime show-timezone year
service timestamps debug datetime msec localtime show-timezone year
```

Finally, NSA also recommends enabling log messages to indicate when a user was successful or unsuccessful at logging into the system. Even though these events are recorded on the centralized AAA servers when accounting is properly configured, this information is not logged in the local buffer. Ensure these events are logged with the following configuration commands:

```
login on-failure log
login on-success log
```

6.4 Synchronize clocks

The Network Time Protocol (NTP) is used to synchronize device clocks worldwide and to ensure that the timestamps included with log messages are reasonably accurate. To provide this reliability, each device should synchronize with at least two trusted time sources. This accuracy is critical to ensure log message timestamps can be easily correlated across geographically dispersed time zones, and used to collectively trace a network incident from one device to another.

NSA recommends that each device and the remote log servers use at least two trustworthy and reliable time servers to ensure accuracy and availability of information. Internal time servers should be established as the primary source for all devices, which should subsequently synchronize with authoritative external sources. This design decreases the number of external requests and ensures consistency of timestamps in

the event an external time server is unreachable. When deploying time servers on the network, administrators should confirm that devices are able to access the time servers, and that the clocks are synchronized after the configuration has been applied.

NSA also recommends enabling NTP authentication on all devices to prevent clock tampering, and configuring strong, unique NTP authentication keys between the devices and their specified time source.

Establish the trusted NTP keys and enable NTP authentication with the following configuration commands:

```
ntp authentication-key <#1> md5 <KEY>
ntp trusted-key <#1>
ntp authentication-key <#2> md5 <KEY>
ntp trusted-key <#2>
ntp authenticate
```

Any number of trusted keys can be established. Note that NTP authentication keys will be stored in the configuration as Type 7 passwords. Type 6 AES-encrypted passwords are not supported for NTP authentication.

Synchronize the device with at least two different NTP servers with the following configuration commands:

```
ntp server <IP_ADDRESS_1> key <#1>
ntp server <IP_ADDRESS_2> key <#2>
```

Note: The number at the end of each command is the trusted NTP key used to authenticate that particular server.

After waiting for the clock to synchronize, verify synchronization and status of the NTP servers with the following exec commands:

```
show ntp status
show ntp associations
```

Note: It is necessary to verify clock synchronization after every NTP configuration change, and it may take several hours for proper synchronization.

Return to Contents

7. Remote administration and network services

Protect your network management tools from adversaries.

Network devices can be managed remotely by administrators through various services. Some common network services include SSH, Hypertext Transfer Protocol (HTTP), SNMP, and File Transfer Protocol (FTP). These services are useful for administrators, but they are also targeted by adversaries to exploit and gain privileged level access to a device. All of them must be properly configured to reduce the probability of a compromise.

7.1 Disable clear text administration services

Clear text protocols pass traffic across the network "in the clear" (i.e., unencrypted) and were designed prior to widespread use of encryption. Therefore, use of these protocols to remotely administer critical devices may lead to an information disclosure that could adversely affect device and network security. An adversary could compromise the network, collecting usernames, passwords, configuration information, and other sensitive data through common information retrieval techniques (e.g., network analyzer or packet capture utility).

NSA recommends using encrypted services to protect network communications and disabling all clear text administration services (e.g., Telnet, HTTP, FTP, SNMP 1/2c). This ensures that sensitive information cannot be easily obtained by an adversary capturing network traffic. For detailed information on how to enable encrypted services, refer to 7.11 Network service configurations.

If a device does not support encrypted protocols, connect a management system directly to the console or management port, or establish a dedicated out-of-band management network to reduce the ability of an adversary capturing the clear text protocols. Disable the Telnet service with the following configuration commands:

```
line vty 0 4
 transport input none

line vty 5 15
 transport input none
```

Depending on the device, it may be necessary to apply a similar configuration to other lines as well. If VTY lines 5 through 15 do not exist on a particular device, it is not

necessary to execute those commands. Note that these commands may also disable other services that are enabled on the lines by default, including SSH. For detailed information on how to enable SSH, refer to 7.11.1 Network service configurations SSH.

Disable the HTTP service with the following configuration command:

```
no ip http server
```

For detailed information on how to enable the secure HTTP service, refer to 7.11.2 Network service configurations HTTP.

Disable versions 1 and 2c of the SNMP and SNMP trap services by removing any configured community strings with the following configuration commands:

```
no snmp-server community <COMMUNITY_STRING>
no snmp-server host <HOSTNAME_OR_IP_ADDRESS> <COMMUNITY_STRING>
```

For detailed information on how to enable SNMP version 3, refer to 7.11.3 Network service configurations SNMP.

Disable the Trivial File Transfer Protocol (TFTP) by removing any lines with the following configuration command:

```
no tftp-server <FILENAME>
```

The FTP service is generally not enabled as a listening service, but the protocol can be used as a client. Remove FTP credentials with the following configuration commands:

```
no ip ftp username
no ip ftp password
```

7.2 Ensure adequate encryption strength

Some encrypted services require that a public and private key pair be generated so clients can connect and authenticate to the server. Additionally, the client and server of an encrypted connection may collectively establish a private session key for each unique connection. Encrypted connections that use weak algorithms or a small number of bits make it easier for an adversary to crack the private session key and decrypt all of the data transferred during a unique connection.

For guidance on which algorithms and ciphers are NSA-approved for National Security Systems (NSS), refer to CNSSP 15 [4]. The CNSSP 15 requirements are explained in the draft IETF documents on Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec), Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3, and Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell (SSH) [5], [15], [16].

For related requirements and guidance for non-NSS U.S. Government systems, refer to NIST SP 800-52 Revision 2 Appendix F [17].

These documents contain the latest recommended encryption parameters.

NSA recommends that 3072 bits or higher be used for asymmetric (public and private) key generation, 384 bits for elliptic curve cryptography (ECC) keys, and 256 bits for symmetric encryption keys. Some systems may not support 3072 bits, so it may be necessary to use 4096 bits instead. For any device that has a smaller key size, regenerate a new key pair and configure encrypted protocols to only use approved algorithms. A larger key size may increase the time to connect to the service (due to extra computations), but is negligible on most devices. For more information on configuring encrypted services, refer to 7.11 Network service configurations.

7.3 Utilize secure protocols

Several common administration services implement protocols that contain flaws in the implementation and exchange of information, which can be exploited by an adversary. Some protocols, such as SSH, can be configured to be backward compatible and accept older insecure protocols, along with the newer ones. Older protocols are subject to man-in-the-middle techniques that can force clients and servers to negotiate weaker algorithms, possibly without user awareness.

NSA recommends ensuring administration services are using the latest version of protocols, with the proper security settings adequately enabled. SSH version 2 is the preferred method for remotely accessing devices. Encrypted HTTP servers should be configured to only accept Transport Layer Security (TLS) version 1.2 or higher. For more information on limiting services to specific versions of the protocol, refer to 7.11 Network service configurations.

7.4 Limit access to services

If a large number of devices are permitted to connect to management services, they are more vulnerable to exploitation. NSA recommends configuring ACLs to allow only administrator systems to connect to devices for remote management. Devices that do not have the capability to support ACLs should be placed on a separate network management segment (e.g. VLAN). Once created, an ACL should be applied to that VLAN or at the ingress router to restrict access to this network segment. It may be necessary to implement a separate firewall in front of critical network segments to restrict what systems can connect to that VLAN. Consider an alternative to using Dynamic Host Configuration Protocol (DHCP); assign administrator systems with static IP addresses or use a smaller pool of addresses. Static addresses will make it easier to define the ACL and limit administrative access to the management services.

Most management services only accept standard ACLs. More than one device or network can be listed on additional lines with the `permit` keyword. Even though every ACL has an implied `deny` statement at the end, it is a best practice to explicitly include it so denied attempts are logged. Create a standard ACL to only permit IP addresses used by administrators with the following configuration commands:

```
access-list <ACL#> permit <NETWORK> <WILDCARD_MASK> log
access-list <ACL#> deny any log
```

For more information on how to apply ACLs to specific administrative services, refer to 7.11 Network service configurations.

NSA also recommends removing unused ACLs from the configuration since they can confuse an administrator into thinking they are properly applied when they are not. After verifying that a standard ACL is not applied, remove it with the following configuration command:

```
no access-list <ACL#>
```

7.5 Set acceptable timeout period

Setting a timeout period for idle connections allows sessions to close after a prescribed time of inactivity. When timeout periods are not set or set too long, it is possible for idle connections to continue indefinitely or even cause a DoS if limited simultaneous connections have been set on the device. The DoS will persist until the idle timeout

period has been reached, which could be indefinite if the idle timeout has been disabled. A longer timeout period provides an adversary with more time to hijack a session while it is idle.

NSA recommends setting the session timeout for administrative connections to five minutes or less on all remote devices (e.g., exec-timeout on VTY lines, SSH, console and auxiliary ports). Do not set the timeout period to zero, as most devices will disable the timeout function with this setting. For more information on limiting the session timeout on specific administrative services, refer to 7.11 Network service configurations.

7.6 Enable Transmission Control Protocol (TCP) keep-alive

TCP keep-alive messages sent and received from a device allow it to assess the connection status when no activity has occurred in a given timeframe. These messages can be used to detect an inadvertent loss in connection and mitigate against potential network compromises. On some devices, the lack of a TCP keep-alive service causes established TCP connections to remain open after an inadvertent connection loss on one end, leaving the session vulnerable to hijacking. Additionally, authentication may not even be required, especially for unencrypted connections, and the adversary could simply resume the session, possibly gaining privileged level access.

NSA recommends enabling TCP keep-alive settings for both inbound and outbound messages for all TCP connections with the following configuration commands:

```
service tcp-keepalives-in
service tcp-keepalives-out
```

Note that some devices do not support the configuration of TCP keep-alive messages.

7.7 Disable outbound connections

After authenticating to a device via a management port, a user generally has the ability to remotely connect to other systems on the network through supported protocols (e.g., Telnet and SSH). If an adversary was able to compromise the device or use an administrator account to gain user level access, this outbound connection could potentially be used to advance through the network. Properly reviewing device configurations and leveraging ACLs can prevent unauthorized systems from accessing network resources.

NSA recommends disabling outbound connections to limit an adversary from moving through the network with the following configuration commands:

```
line con 0
 transport output none

line vty 0 4
 transport output none

line vty 5 15
 transport output none
```

Depending on the device, it may be necessary to apply a similar configuration to other lines as well. If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands. It is critical to note that this feature must be explicitly disabled on the console line.

If outbound connections are required for copying files to or from the devices for maintenance or integrity verification, restrict it to only SSH and limit the number of devices that can be accessed via outbound ACLs; revert to the above configuration once the task is complete.

7.8 Remove SNMP read-write community strings

An SNMP version 1 or 2c read-write community string is similar to a password, and can be used to access or modify device configurations and operating system files. These actions generally cannot be done with a read-only community string. Because SNMP read-write community strings are sent in clear text, they can be exploited by an adversary to gain complete control of a network device.

NSA recommends removing all SNMP read-write community strings and upgrading to SNMP version 3 with encryption and authentication. If a version 1 or 2c SNMP read-write community string is required for remote administration and cannot be removed, it is recommended that the read-write community string be significantly different from other community strings to prevent an adversary from guessing the read-write community string if a read-only community string is obtained.

All version 1 and 2c SNMP community strings can be listed with the following exec command:

```
show running-config | include snmp-server community
```

Note: A read-write community string will include the `RW` keyword, while a read-only community string will include the `RO` keyword.

Disable an SNMP read-write community string with the following configuration command:

```
no snmp-server community <COMMUNITY_STRING>
```

7.9 Disable unnecessary network services

During the initial installation of devices, several TCP and UDP services are enabled by default, even though the provided networking features are unnecessary for normal operations. These services can degrade the security level of the network, offering an adversary additional access points to exploit a device and leave it susceptible to unauthorized monitoring, information gathering, and compromise.

For example, Cisco Smart Install is often unnecessary, but when left enabled, an unauthenticated remote adversary could use this service to obtain a device's configuration file, upload a new configuration or operating system image file, or force a reboot. This has been documented in Cisco's security advisory cisco-sa-20170214-smi as a misuse of the protocol, but the security community has observed and acknowledged this issue as a severe vulnerability exploited by adversaries to obtain configuration files across the Internet [18], [19].

NSA recommends disabling every unnecessary service on each device. If the service is required and can support a password and ACLs, create a password based on NSA's strong password guidance (see 5.6 Create strong passwords) and apply an ACL to only allow required systems to connect to the service. If a device does not support ACLs, it can be moved to a separate VLAN, and an ACL can be applied to the VLAN.

NSA also recommends immediately disabling the Cisco Smart Install service on all devices with the following configuration command:

```
no vstack
```

Even though this service is designed for switches, routers can also be configured as a Cisco Smart Install director; therefore, it should be explicitly disabled on all devices, especially when they are first configured.

Disable other unnecessary TCP and UDP services with the following configuration commands:

```
no service tcp-small-servers
no service udp-small-servers
no service finger
```

7.10 Disable discovery protocols on specific interfaces

Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) are broadcast protocols that periodically advertise network topology and device information to neighboring devices that support the protocol and are listening for packets. This functionality is enabled by default and can be useful for administrators to obtain information about the network, but it is also extremely useful to an adversary who can passively gather network configuration information. An adversary that is able to deploy a sniffer in a network could collect device model numbers, operating system versions, VLAN information, and physical and logical addresses, gaining valuable information to exploit devices on the network.

NSA recommends disabling CDP and LLDP on all devices capable of using these services. If a service is required for proper network communications (e.g., some Cisco Voice-over-IP (VoIP) phones), only enable it on point-to-point links between devices that require the protocol or on voice enabled ports.

CDP and LLDP can be globally disabled with the following configuration commands:

```
no cdp run

no lldp run
```

If CDP is required on specific interfaces, it must be globally enabled but disabled on all other interfaces, as shown in the following configuration commands for a single interface:

```
interface <INTERFACE>
 no cdp enable
```

7.11 Network service configurations

This section describes how to properly enable common remote network administration services.

7.11.1 SSH

Allow inbound SSH connections with the following configuration commands:

```
line vty 0 4
 transport input ssh

line vty 5 15
 transport input ssh
```

Note: This may disable other services enabled on the lines by default, such as Telnet. If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands. Depending on the device, it may be necessary to apply a similar configuration to other lines as well.

Allowed input transports can be confirmed with the following exec command:

```
show line <LINE> <LINE_NUMBER>
```

Disable SSH version 1 connections and only allow version 2 of the protocol with the following configuration command:

```
ip ssh version 2
```

Generate a new asymmetric Rivest-Shamir-Adleman (RSA) key pair for SSH with the following configuration command:

```
crypto key generate rsa modulus 3072
```

Note: This command will overwrite an existing RSA key pair.

Generate a new asymmetric ECC key pair for SSH with the following configuration command:

```
crypto key generate ec keysize 384
```

Note: This command will overwrite an existing ECC key pair.

Set the minimum Diffie-Hellman key size to 4096 bits with the following configuration command:

```
ip ssh dh min 4096
```

Note: Some systems do not support 3072 bits for the Diffie-Hellman key size, so 4096 bits is recommended.

The encryption, key exchange (KEX), and message authentication code algorithms accepted by the SSH protocol can be specified (to include the preferred order) with the following configuration commands:

```
ip ssh server algorithm encryption <ALGORITHM> [<ALGORITHM> ...]
ip ssh server algorithm kex <ALGORITHM> [<ALGORITHM> ...]
ip ssh server algorithm mac <ALGORITHM> [<ALGORITHM> ...]
```

For more information on acceptable algorithms, refer to CNSSP 15 [4]. The CNSSP 15 requirements are explained in the draft IETF document on Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell (SSH) [16].

The configuration of the SSH service can be confirmed with the following exec command:

```
show ip ssh
```

Apply a standard ACL to only permit IP addresses used by administrators with the following configuration commands:

```
line vty 0 4
 access-class <ACL#> in

line vty 5 15
 access-class <ACL#> in
```

If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands. Note that this ACL would also apply to Telnet if it was enabled on the lines. Depending on the device, it may be necessary to apply a similar configuration to other lines as well. Refer to 7.4 Limit access to services for more information on creating a standard ACL.

Set the session expiration to 5 minutes or less with the following configuration commands:

```
line con 0
 exec-timeout 5 0
```

```
line vty 0 4
 exec-timeout 5 0

line vty 5 15
 exec-timeout 5 0
```

If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands. Note that this would also apply to Telnet if it was enabled on the lines. Depending on the device, it may be necessary to apply a similar configuration to other lines as well.

7.11.2 HTTP

If HTTP is used for management purposes, enable HTTP over TLS with the following configuration command:

```
ip http secure-server
```

Only accept TLS version 1.2 with the following configuration command:

```
ip http tls-version TLSv1.2
```

The cipher suites accepted by the encrypted HTTP service can be specified (to include the preferred order) with the following configuration command:

```
ip http secure-ciphersuite <CIPHERSUITE> [<CIPHERSUITE> ...]
```

For more information on acceptable algorithms, refer to CNSSP 15 [4]. The CNSSP 15 requirements are explained in the draft IETF document on Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3 [15].

Apply a standard ACL to only permit IP addresses used by administrators with the following configuration command:

```
ip http access-class <ACL#>
```

Note: This ACL would also apply to the clear text HTTP service if it was enabled. For more information on creating a standard ACL, refer to 7.4 Limit access to services.

The default idle timeout of an HTTP server connection is 180 seconds (three minutes), so it is not necessary to change this value.

7.11.3 SNMP

If SNMP is used for management, enable SNMP version 3 with both authentication and privacy (encryption) with the following configuration commands:

```
snmp-server group <SNMPv3_GROUP> v3 priv access <ACL#>
snmp-server user <USER> <SNMPv3_GROUP> v3 auth sha <AUTH_PASSWORD> priv aes
 256 <PRIV_PASSWORD> access <ACL#>
```

First a group must be defined, where the `priv` keyword is equivalent to authPriv (both authentication and privacy). One or more users must be defined and assigned to a group. In addition to the authentication and encryption parameters, two different passwords must be supplied for each user, one for authentication and one for privacy. Interoperability issues have been observed with AES-192 and AES-256, so it may be necessary to use AES-128 for encryption instead of AES-256 with the `aes 128` keywords. As shown above, an ACL can be applied to both the group and each individual user by specifying it as a separate option at the end of each command with the `access` keyword.

The above SNMP configuration can be tested from a Linux system with the following shell command:

```
snmpget -v 3 -u <USER> -a sha -l authPriv -A '<AUTH_PASSWORD>' -x AES \
 -X '<PRIV_PASSWORD>' <IP_ADDRESS> 1.3.6.1.2.1.1.5.0
```

Return to Contents

8. Routing

Routers forward data packets between computer networks. When a router receives a packet, it uses its routing table and the packet's network address information to determine the next hop to reach its destination. An improper configuration of the router itself or the dynamic routing protocols used to populate the routing table could allow an adversary to redirect packets to a different destination, allowing sensitive data to be collected, manipulated, or discarded, which would violate confidentiality, integrity, or availability.

Configure your routers for network use vs. malicious abuse.

8.1 Disable IP source routing

IP source routing is a rarely used feature that enables the sender of a packet to specify a pre-determined list of intermediate nodes where it should be forwarded rather than using the internal routing table to make a decision. Leveraging this setting, an adversary could transmit packets through a route of their choosing. Along with IP address spoofing, an adversary can use the IP source routing feature to successfully bypass ACLs and other network restrictions, essentially choosing its own network path. Although this vulnerability is associated with routers and how packets are routed, the functionality can also be exploited on switches.

NSA recommends disabling IP source routing on all devices, not just routers, since this feature is not required for normal network operations. Depending on the vendor of a product, it may be necessary to disable forwarding of each IP source route option individually. A similar feature is available in IPv6, and needs to be disabled separately. Disable IP source routing with the following configuration commands:

```
no ip source-route
no ipv6 source-route
```

8.2 Enable unicast reverse-path forwarding (uRPF)

uRPF is a method of protection against IP spoofing that instructs a router to examine both the source and destination addresses in the packet. When a packet is received on an interface, the source address is compared to entries in the routing table and is forwarded if the return route matches where the packet was received. Otherwise, it is discarded due to concerns that the source address in the packet may have been spoofed. If uRPF is not enabled, an adversary may be able to successfully spoof the source address of IP packets sent into the network.

NSA recommends enabling uRPF on external interfaces of perimeter routers. On routers, it is necessary for Cisco Express Forwarding (CEF), which provides optimized lookups for efficient packet forwarding, to be enabled before uRPF. Note that uRPF should not be enabled on internal interfaces or routers that have asymmetrical routing (where two or more return routes may exist for a given source address), as this situation could cause legitimate packets to be discarded. Enable uRPF on a single interface with the following configuration commands:

```
ip cef
interface <INTERFACE>
 ip verify unicast reverse-path
```

8.3 Enable routing authentication

Dynamic routing protocols are used to distribute information to neighboring devices and provide routes to reach other networks. Network devices will use this information to populate their own routing table, which is then used to determine the next hop for forwarding a packet to the requested destination. To control the flow of traffic, an adversary may inject, modify, or corrupt the routing information sent and received by neighboring devices. To prevent route manipulation, routing authentication should be enabled to ensure the routing information received from neighboring devices has not been manipulated by an untrusted source.

NSA recommends enabling routing authentication on any dynamic routing protocols used that receive routing updates from other devices on the network. Enable Open Shortest Path First (OSPF) routing authentication by enabling it on the OSPF process for each area and applying the authentication key to each interface associated with that process with the following configuration commands:

```
key chain <KEY_CHAIN_NAME>
 key <KEY_NUMBER>
 key-string <KEY>
 cryptographic-algorithm hmac-sha-512

interface <INTERFACE>
 ip ospf authentication key-chain <KEY_CHAIN_NAME>
```

NSA also recommends using a unique key between all neighbors, instead of using the same authentication key for all interfaces on all devices. If the keys are different, an adversary would not be able to use a compromised key from one network to inject a malicious route on another network.

Enable Border Gateway Protocol (BGP) routing authentication by applying a unique password key to each individual peer with the following configuration commands:

```
router bgp <AS_NUMBER>
 peer <IP_ADDRESS_1> password <KEY>
```

Enable Enhanced Interior Gateway Routing Protocol (EIGRP) authentication by creating a key-chain and applying it to each interface with the following configuration commands:

```
key chain <KEY_CHAIN_NAME>
 key <KEY_NUMBER>
  key-string <KEY>
  cryptographic-algorithm hmac-sha-512

interface <INTERFACE>
 ip authentication key-chain eigrp <AS_NUMBER> <KEY_CHAIN_NAME>
```

Note: An arbitrary name and number can be chosen for each key. The *<KEY>* is the shared key assigned to neighboring devices. The `cryptographic-algorithm` can also be set to `hmac-sha-384` and still meet CNSSP 15 guidance [4].

Do not use the Routing Information Protocol (RIP). It is slow to converge, does not scale, and RIP version 1 cannot be configured to authenticate nearby routers, making it easy for an adversary to exploit the protocol. Devices that only support RIP should use static or default routes to other devices that support modern routing protocols with authentication.

Return to Contents

9. Interface ports

The interface ports of network switches physically connect workstations, servers, and other devices to the network, while the interconnections between routers and switches define how systems communicate across the network. An adversary must first obtain physical access to the network to connect an unauthorized system, or use a system already established on the network to exploit an existing connection. Properly configured interface ports can prevent an adversary from performing exploitation attempts against the network.

Prevent an adversary from connecting to your network.

9.1 Disable dynamic trunking

A trunk is a point-to-point link between two devices that exchange VLAN encapsulated frames. Depending on the traffic being sent over the link, it is possible for an interface port to dynamically configure itself to be either a trunk or an access port. An adversary

that is connected to a dynamic port could instruct it to become a trunk port and potentially gain access to network traffic without regard to VLAN separation.

NSA recommends disabling dynamic trunking as it is not necessary for an interface port to dynamically configure itself. When a device is added to the network, ensure that all interface ports are explicitly configured as either trunk ports or access ports. Systems that do not handle VLAN encapsulated frames should be connected to a port that is configured for access only.

Strictly configure an interface port for static access only with the following configuration commands:

```
interface <INTERFACE>
 switchport mode access
```

Strictly configure an interface port to be a trunk with the following configuration commands:

```
interface <INTERFACE>
 switchport mode trunk
```

9.2 Enable port security

Physical interface ports of devices are often the last line of defense and a primary means of restricting access to a network. Port security limits the number of valid MAC addresses allowed to connect to a switchport, restricting connectivity only to those authorized. A switchport not configured to enforce port security could allow an adversary with physical access to connect an unauthorized system. The adversary could then act as a trusted system and bypass existing security restrictions, gathering network information, probing deeper into the network, or compromising internal systems.

NSA recommends enabling port security on all active switchports on a device, and setting the maximum number of allowed MAC addresses for each port to be exactly one, or two if VoIP capabilities are in use. Port security is not a replacement for a NAC, such as 802.1X, but should be used when a NAC cannot be implemented. If possible, assign a fixed MAC address to each switchport that is connected to a known system, and configure each switchport to either shutdown or send an SNMP trap message when a port security violation occurs. Port security can be enabled on trunk interfaces;

however, it is not recommended as it requires knowing the number of devices that have traffic traversing that specific trunk. A dynamic switchport cannot have port security enabled simultaneously, and must first be configured for static access before port security can be enabled.

Enable port security on a static access port with a maximum of one MAC address with the following configuration commands:

```
interface <INTERFACE>
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
```

The `sticky` keyword will allow the device to insert the MAC address in the configuration once the first authorized system is connected to that port. Note that the configuration will need to be saved to retain the information after a reboot. If shutting down a port is not an acceptable action because of availability concerns, the `shutdown` keyword can be replaced with `restrict` to prevent any additional MAC addresses from communicating on that port.

9.3 Disable default VLAN

Most switches utilize VLAN 1 as the default, including management ports, which may provide direct access to the switch for administration. Additionally, some layer 2 protocols (e.g., discovery or trunking) need to be sent on a specific VLAN on trunk links, and VLAN 1 is generally selected as the default. If mitigation steps are not taken, the default VLAN may span the entire network, and place trusted devices at a higher security risk of exploitation by untrusted devices that gain access.

NSA recommends moving all management and operational traffic to different VLANs (not the default) that separate management traffic from user data and protocol traffic, and using multiple switches to separate different security levels of network traffic. The default VLAN should also be logically disallowed on all trunks and access ports that don't require it (including disconnected and shutdown ports) to ensure it does not transmit unnecessary broadcast, multicast, and unknown destination traffic.

Frames that are sent and received on trunk ports are usually tagged with the VLAN ID associated with the frame. Any frames received that are not tagged are automatically

placed in the native trunking VLAN associated with that port. The native trunking VLAN should be assigned the same on both ends of a trunk link. Similarly, frames that are sent and received on access ports are assigned to the access VLAN associated with that port. All switchports are assigned to an access VLAN and a native trunking VLAN, regardless if they are trunk or access ports.

NSA recommends assigning all trunk ports to a unique native trunking VLAN that is only assigned to trunk ports, and assigning the access VLAN to an unused and disabled VLAN. Similarly, NSA recommends assigning all access ports to the appropriate access VLAN, and assigning the native trunking VLAN to another unused and disabled VLAN, different from the ones used by trunk ports. This configuration will prevent an adversary from jumping between active VLANs by intentionally tagging traffic that would otherwise be untagged.

Create a unique trunking VLAN (500) and an unused and disabled access VLAN (997), both assigned to a trunk port, with the following example configuration commands:

```
vlan 500
 name NATIVE-TRUNK

vlan 997
 name UNUSED-ACCESS
 shutdown

interface <INTERFACE>
 switchport mode trunk
 switchport access vlan 997
 switchport trunk native vlan 500
 switchport trunk allowed vlan 2-4094
```

This configuration also allows all VLANs, except for the default VLAN 1, to traverse the trunk. If all configured VLANs are known, NSA recommends allowing only those specific VLANs, rather than just excluding VLAN 1.

Create an unused and disabled VLAN (998), assigned to the native trunking VLAN of an access port, with the following example configuration commands:

```
vlan 998
 name UNUSED-NATIVE
 shutdown
```

```
interface <INTERFACE>
 switchport mode access
 switchport access vlan <ACCESS_VLAN#>
 switchport trunk native vlan 998
```

Switchports can also be assigned a third VLAN, if VoIP capabilities are in use, with the following configuration commands:

```
interface <INTERFACE>
 switchport voice vlan <VOICE_VLAN#>
```

All of the VLANs associated with individual switchports can be confirmed with the following exec command:

```
show interfaces switchport
```

9.4 Disable unused ports

Leaving unused ports enabled on a device allows an adversary to attach a rogue device to the network and perform information gathering or compromise attempts. All unused ports should be disabled and placed in an unused VLAN, which is not the default.

NSA recommends disabling all unused ports on a device by shutting down the associated interfaces and, if supported by the device, assigning unused ports to an unused VLAN. This will continue to prevent access to the network, even if the ports become enabled. Prior to disabling a port, it is necessary to verify that it is truly unused and nothing is connected. If a device connected to the port is powered off, it may appear that the switchport is unused.

Shut down all unused interfaces and assign the access and native trunking VLANs to unused and disabled VLANs with the following example configuration commands:

```
vlan 999
 name UNUSED-DISABLED
 shutdown

interface <INTERFACE>
 switchport mode access
 switchport access vlan 999
 switchport trunk native vlan 998
 no switchport voice vlan
 shutdown
```

Note: It is not necessary to assign the voice VLAN to an unused VLAN, as it will remain unassigned if VoIP capabilities are not in use.

9.5 Disable port monitoring

Port monitoring is used on a network switch to send a copy of network packets seen on one switchport to a network monitoring connection on another switchport. A device that has one or more port monitoring sessions defined allows a set of source ports to be monitored by a specified destination port, and all traffic being sent to or from the source ports will also be sent to the destination port. Port monitoring is typically used for connecting an NIDS, diagnosing a problem, or using a network analyzer to monitor the network. Depending on the vendor, port monitoring is also known as "port mirroring" or "port spanning." An adversary connected to the destination port of a port monitoring session will be able to collect network traffic sent through all the source ports specified by the session.

NSA recommends disabling all inactive port monitoring sessions on a device. Port monitoring should only be enabled for those ports where it is necessary, and should be disabled once they are no longer needed. Examples of this necessity are an NIDS or an administrator monitoring the network.

Note: Some vendors do not allow traffic to be sent from the destination port of a port monitoring session, effectively disabling network access from that port. This type of behavior is desired when an NIDS is connected to a port monitoring session.

List the monitoring sessions defined in the configuration with the following exec command:

```
show monitor session [1|2|all]
```

Note: If the `all` keyword is supported, it will list all of the defined sessions; otherwise each individual session number will need to be specified in separate commands, generally `1` and `2`.

Remove a monitoring session defined in the configuration with the following configuration command:

```
no monitor session <SESSION#>
```

9.6 Disable proxy Address Resolution Protocol (ARP)

Proxy ARP is a technique in which a proxy server on a network answers ARP requests for an IP address that is not on that network. It helps devices on a subnet reach remote subnets, without configuring routing on a default gateway. It can be advantageous since it can be added to a router without disbursing routing tables from other networks, but is only safe between trusted local area network (LAN) segments. This technique introduces vulnerabilities into the network as adversaries can spoof a trusted system and intercept packets.

NSA recommends disabling proxy ARP on all interfaces unless the device is being used as a LAN bridge or to allow inbound network address translations (NAT) for multiple destination IP addresses. It may be necessary to disable proxy ARP on each individual interface, rather than disabling it globally.

Find interfaces that have proxy ARP enabled with the following exec command:

```
show ip interface
```

Disable Proxy ARP on an individual interface with the following configuration commands:

```
interface <INTERFACE>
 no ip proxy-arp
```

Return to Contents

10. Notification and consent banners

The technical recommendations provided in this document can significantly reduce the probability of an adversary exploiting a vulnerability on the network. Unfortunately, an adversary or insider may still be able to find a weakness to compromise, circumvent, or disrupt the network. Having a notification banner can make clear what is permissible to anyone who accesses the system, and add any necessary notices and disclaimers.

Display notifications of authorized use and consent to monitoring.

10.1 Present a notification banner

Depending on the organization's requirements, a notification banner can provide notice to users that connecting to the network device is for authorized use only and that any use of the system is subject to monitoring for any authorized purpose. A legally sufficient banner ensures the network owner and others, including the Government, can take necessary steps to monitor and secure the network. However, the precise requirements for such a banner will vary by organization and jurisdiction. For example, DoD elements must use a banner that meets the requirements of DoD Instruction 8500.01. Other U.S. Government entities should implement the requirements of NIST SP800-53, AC-8. For private sector entities, the Cybersecurity and Infrastructure Security Agency has issued very helpful guidance on developing an appropriate banner [20].

NSA recommends that each device be configured to present the full notification banner whenever a user logs into an information system or connects to any remote service.

Cisco IOS devices have two types of banners; the login banner is displayed prior to a user logging in, and then the "message of the day" is displayed after the user successfully authenticates. At a minimum, the notification banner should be displayed to both authorized and unauthorized users attempting to login. The same or additional information could be provided to authenticated users after logging in, if desired.

Add a notification banner, with the organization's banner appropriately inserted, prior to users logging in with the following configuration command:

```
banner login ^
INSERT NOTIFICATION BANNER HERE
^
```

Note: The caret symbol ("^") is used as a delimiter so the banner can span multiple lines, assuming the caret symbol is not used in the banner itself. After this command is inserted into the configuration, the delimiter will generally appear as "^C" instead of "^". Do not type in "^C" as part of the command, otherwise the banner will begin with a "C".

Add the same notification banner or additional information for authorized users who have successfully authenticated with the following configuration command:

```
banner motd ^
INSERT NOTIFICATION BANNER HERE
ADDITIONAL INFORMATION
^
```

Return to Contents

11. Conclusion

The guidance in this report was generated from a depth and breadth of experience in assisting NSA customers with evaluating their networks and providing recommendations to immediately harden network devices. Along with essential maintenance functions, administrators play a critical role in defending networks against adversarial threats. Following this guidance will assist these network defenders with putting cybersecurity best practices into action, lowering the risk against compromise and ensuring a more secure and better protected network.

Acronyms

AAA	Authentication, authorization, and accounting
ACL	Access control list
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AUX	Auxiliary
BGP	Border Gateway Protocol
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CISA	Cybersecurity and Infrastructure Security Agency
CNSA	Commercial National Security Algorithm Suite
CNSSP	Committee on National Security Systems Policy
CON	Console
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized zone
DoS	Denial of service
ECC	Elliptic curve cryptography
ECP	Elliptic curve group modulo a prime
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IP	Internet Protocol
IPS	Intrusion prevention system
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet service provider
KEX	Key exchange
LAN	Local area network
LLDP	Link Layer Discovery Protocol
MAC	Media access control
MD5	Message Digest 5
MODP	Modular Exponent
NAC	Network access control
NAT	Network address translation
NDI	Network Device Integrity
NIDS	Network intrusion detection system
NIST	National Institute of Standards and Technology
NSA	National Security Agency

NSS	National Security System(s)
NTP	Network Time Protocol
OMB	Office of Management and Budget
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
RSA	Rivest-Shamir-Adleman
SCP	Secure Copy Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIEM	Security information and event management
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
uRPF	Unicast reverse-path forwarding
UTC	Coordinated Universal Time
VLAN	Virtual local area network
VoIP	Voice over IP
VPN	Virtual private network
VTY	Virtual teletype

References

Works cited

[1] Cybersecurity and Infrastructure Security Agency (2022), Layering Network Security Through Segmentation. Available at: https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf

[2] National Security Agency (2019), Segment Networks and Deploy Application-aware Defenses. Available at: https://www.nsa.gov/cybersecurity-guidance

[3] National Security Agency (2021), Selecting and Hardening Remote Access VPN Solutions. Available at: https://www.nsa.gov/cybersecurity-guidance

[4] Committee on National Security Systems (2016), CNSS Policy 15. Available at: https://www.cnss.gov/CNSS/issuances/Policies.cfm

[5] Corcoran, Jenkins, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec). Available at: https://datatracker.ietf.org/doc/html/draft-corcoran-cnsa-ipsec-profile

[6] National Security Agency (2020), Configuring IPsec Virtual Private Networks. Available at: https://www.nsa.gov/cybersecurity-guidance

[7] National Security Agency (2019), Mitigating Recent VPN Vulnerabilities. Available at: https://www.nsa.gov/cybersecurity-guidance

[8] National Security Agency (2021), Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations. Available at: https://www.nsa.gov/cybersecurity-guidance

[9] Cisco Systems, Inc. (2022), Support & Downloads. Available at: https://www.cisco.com/c/en/us/support/index.html

[10] National Security Agency (2016), Network Device Integrity (NDI) Methodology. Available at: https://www.iad.gov/iad/library/reports/network-device-integrity-methodology.cfm

[11] National Security Agency (2016), Network Device Integrity (NDI) on Cisco IOS devices. Available at: https://www.iad.gov/iad/library/reports/network-device-integrity-ndi-cisco-ios-devices.cfm

[12] National Security Agency (2016), Validate Integrity of Hardware and Software. Available at: https://www.iad.gov/iad/library/ia-guidance/security-tips/validate-integrity-of-hardware-and-software.cfm

[13] National Security Agency (2022), Cisco Password Types: Best Practices. Available at: https://www.nsa.gov/cybersecurity-guidance

[14] Office of Management and Budget (2021), Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents. Available at: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

[15] Cooley, D, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3. Available at: https://datatracker.ietf.org/doc/html/draft-cooley-cnsa-dtls-tlsprofile

[16] Gajcowski, Jenkins, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell (SSH). Available at: https://datatracker.ietf.org/doc/html/draft-gajcowski-cnsa-ssh-profile

[17] National Institute for Standards and Technology (2020), Special Publication 800-52 Rev. 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. Available at: https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

[18] Cisco Systems, Inc. (2017), Cisco Smart Install Protocol Misuse. Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi

[19] National Security Agency (2017), Cisco Smart Install Protocol Misuse. Available at: https://www.nsa.gov/cybersecurity-guidance

[20] Cybersecurity and Infrastructure Security Agency (2022), Guidance on Consent Banners. Available at: https://www.cisa.gov/publication/guidance-consent-banners

Related guidance

- Biden (2021), Executive Order 14028: Improving the Nation's Cybersecurity. Available at: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
- National Institute of Standards and Technology (2020), Special Publication 800-207: Zero Trust Architecture. Available at: https://www.nist.gov/publications/zero-trust-architecture
- Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team (2021), Department of Defense (DOD) Zero Trust Reference Architecture. Available at: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf
- National Institute for Standards and Technology (2020), Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management. Available at: https://pages.nist.gov/800-63-3/sp800-63b.html
- National Security Agency (2019), Continuously Hunt for Network Intrusions. Available at: https://www.nsa.gov/cybersecurity-guidance
- National Security Agency (2021), Embracing a Zero Trust Security Model. Available at: https://www.nsa.gov/cybersecurity-guidance
- National Security Agency (2020), Hardening Network Devices. Available at: https://www.nsa.gov/cybersecurity-guidance